



# HIPAA: A Closer Look

Presented By Michelle Bilsky, CHCO, LHRM, MLA, CBA  
Certified HIPAA Compliance Officer

**Med**  **Mal**  
**DIRECT**  
Insuring a Healthy Practice

# What Does HIPAA Mean?

- HIPAA stands for Health Insurance Portability and Accountability Act of 1996.
- This is a federal rule covering the healthcare and health insurance industries.
- Under HIPAA, patient privacy is every healthcare employee's concern.
- HITECH stands for Health Information Technology of Economic and Clinical Health
- HITECH expands privacy and security provisions and penalties to business associates with HIPAA

# HIPAA: A Closer Look



In order to help improve healthcare, HIPAA includes measures for:

- Standardizing how insurance claims are processed
- Making sure health information is transmitted securely
- Protecting the privacy of patients

# Security and Privacy

Security and privacy are key under the Privacy Rule. These two things may seem similar, but there is a difference:

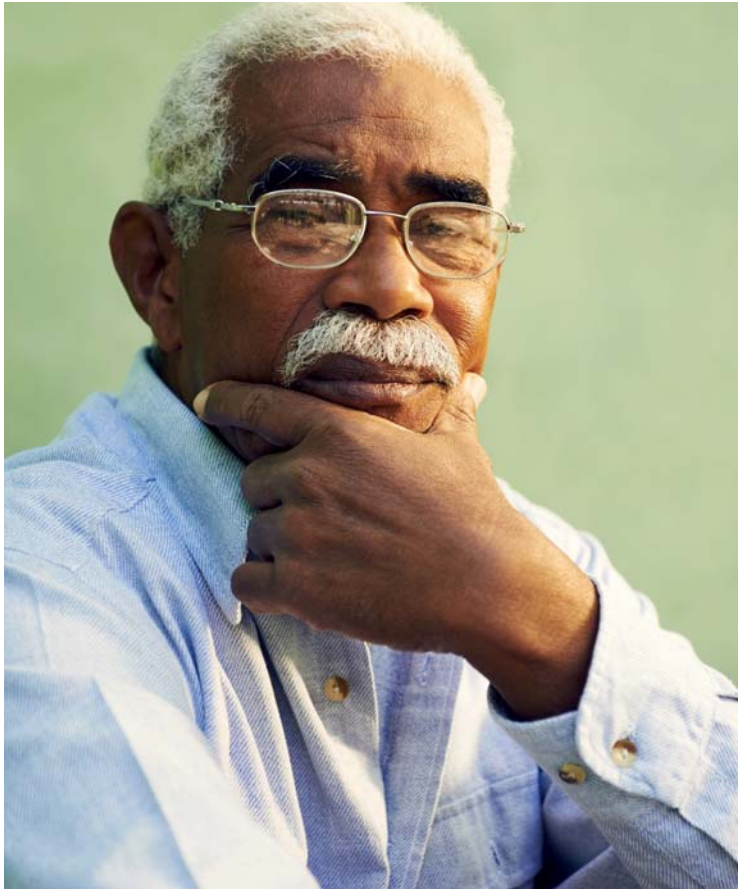


The HIPAA Security Rule covers information that is stored or transmitted electronically—for example, using the Internet or private computer networks.



The HIPAA Privacy Rule covers certain health information in any form.

# Patient Privacy



Patient privacy is everyone's concern. It is a basic part of patient care.

- Standards for Privacy of Individually Identifiable Health Information (The Privacy Rule for short) was created to protect the privacy of healthcare patients.
- HIPAA became law in 1996. The Privacy Rule of HIPAA took effect in April 2001. Most healthcare organizations had to meet the standards set by the rule by April 2003.

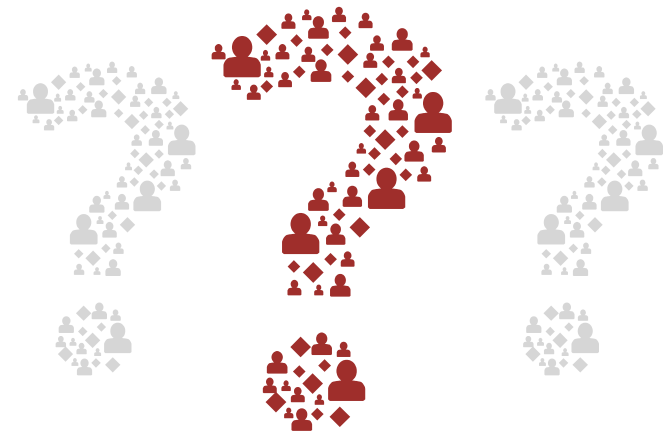
# Who Does the Rule Affect?

The HIPAA Privacy Rule applies to most healthcare organizations that hold or transmit personal health information. These may include: Healthcare providers' offices





- Hospitals
- Laboratories
- Pharmacies
- Radiology Centers
- Home-health agencies
- Healthcare billing services
- Providers of health insurance and HMOs (health maintenance organizations)

# Who Does the Rule Affect?

- Within these organizations, all employees must keep information private. Certain businesses that work with these organizations may have to meet the rule's standards too.
- All Employees need to comply with privacy rules and protect patient information.



## The HIPAA Privacy Rule Allows Patients to:

-  See and get copies of their health records (with some exceptions)
-  Ask for corrections to their health records if they see errors
-  Find out and limit how their personal health information may be used
-  Ask for and receive information about how their personal health information has been used in the past (Accounting of Disclosures)



## Is This Serious?



- An organization can be fined each time it breaks the rule. Fines start at \$1,000 per day with a maximum of \$500,000.
- A person can be fined or sent to prison for willful violation.
- The HIPAA Privacy Rule sets a minimum standard for keeping information private. State laws may have stronger standards.

## The HIPAA Privacy Rule Requires Processes:

- Limiting how personal health information can be used
- Requiring security of health records in paper, electronic or other form
- Letting patients know what their rights are and See/obtain copies of their health records (with some exceptions)
- Ask for corrections to their health records if they see errors
- Find out and limit how their personal health information may be used
- Ask for and receive information about how their personal health information has been used in the past (with some exceptions)

# What is Protected Health Information (PHI):



- Health information is any information that applies to a health condition now, in the past, or in the future.
- If health information includes data that would allow someone to identify the patient, it is protected health information. For example, the following items are PHI because they contain a patient's name or patient ID number, and information about his or her health:
  - X-rays, lab reports and other test results
  - Prescriptions
  - Health insurance claims and billing records

# Disclosure



- Disclosure means to give out PHI.
- Providing information about a person for the purpose of billing is one example of disclosure.
  - Does this disclosure require an authorization?
- Talking about a patient's condition in a public place is another example.
  - What is incidental vs. breach exposure?

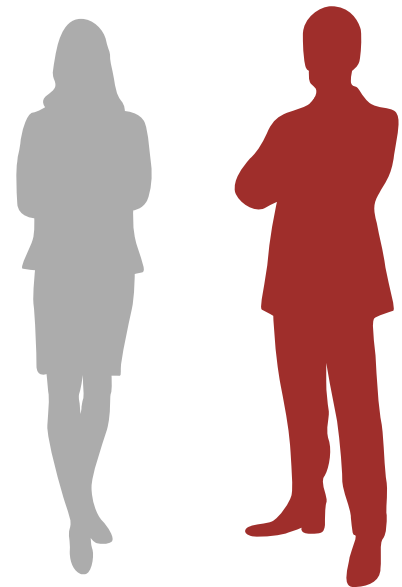
# Minimum Necessary Information

The minimum necessary information is the least information needed in order to get a task or job done.

For Example: The person who sets appointments should not have access to clinical data.

You should:

- Access only the information you need
- Use this information only to do your job
- Limit the information you share with a person to what he or she needs to know in order to do his or her job



# Reasonable Safeguards



- Every Practice must have a written notice of the privacy policy.
- All Employees must know and understand the HIPAA Privacy Rule
- All Employees must make every effort to keep private information private. For example:
  - Do not ask patient for personal info in public (including check in desk)
  - Turn papers upside down and do not leave information where non-staff can read it.

# Written Notice of the Privacy Policy

## Privacy Policy must say:

- That the organization must protect the privacy of the patient
- How the office can use or disclose PHI
- How the office keeps information private
- What the patient's privacy rights are

The notice must be posted in the office waiting room area.

A copy must be offered to all new patients and have them sign that they read it and were offered a copy.

A copy must be available on the covered entities website.

# PHI

Remember, PHI is any health information an organization has or gets from another organization that could be used to identify a specific individual.

Pay attention to information that gives details about who a person is:

- Name
- All or part of an address
- Phone or fax number
- Social Security number
- License plate or driver's license number
- Date of birth
- Admission or discharge date

These are all considered PHI when combined with health information. Health information is protected if it could be used to identify somebody.

- How much information constitutes a breach of PHI?



# Privacy Rule



- The Privacy Rule covers PHI in any format – PHI must be kept private whether it is in written, spoken, or electronic form.
- PHI takes many forms
  - Medical records
  - A prescription label with the patient's name, DOB and the name of the drug
  - A doctor's notes about a patient
  - An X-ray
  - A letter giving patient test results

# Keeping PHI Private



- You must lock filing cabinets and file rooms in which charts are stored
- You must log off computer systems containing patient information when you leave the computer.
- You must shred documents that contain any PHI.

# Using PHI in the Office



If PHI is used publicly, make sure you don't use more than necessary. For example, if you:

- Ask patients to use a sign-in sheet, ask only for their name, and no other identifying information.
- Call out a patient's name in the waiting room, don't reveal any other information about the patient's condition or reason for the visit.

# General Disclosure Information (When Can I Disclose PHI?)

- If it is required by law, such as a court order
- To public health officials, in order to prevent or control disease
- In the case of abuse or domestic violence
- To help law enforcement officials find a suspect, material witness or missing person
- To notify law enforcement officials of a suspicious death
- To funeral directors or coroners
- For the purpose of organ donation
- In the case of some government actions, such as military missions or security activities
- To provide information to meet workers' compensation laws
- To help in disaster relief efforts

In all of these cases, specific conditions apply. You are allowed, but not required, to share information in most of the cases noted here.

# Authorization to Disclose Information

Authorization is permission to use health information

Authorization must be in writing and include specific details about:

What information  
can be used

How the  
information can be  
used

How long the  
information can be  
used

Generally, patients  
can change their  
mind about  
authorization at any  
time.

# Know When Authorization is Required



- One of the goals of the Privacy Rule is to allow patients to have more control over how their health information is used. For example, you must get authorization before:
- Providing information to an insurer or other business for marketing purposes
- Sending the results of a pre-employment physical to an employer

# Consent



- Consent is less formal than authorization. You may get consent to:
- Include a patient in a directory of patients
- Share information with the patient's family or friends
- Use information in ways allowed by the Privacy Rule, such as to treat the patient (TPO).

## EMR/EDI



- Electronic transfers of information
- Information may be sent electronically through email, computer-to-computer faxing or other means. Rules for how information can be transferred electronically come under a different part of HIPAA that deals with security. Healthcare organizations must make sure their systems meet these standards.



# HIPAA Security Rule



- Every organization has its own rules for storing and transferring information, also known as EDI (electronic data interchange). Some key parts to every organization should be the following:
- Use a password –and be sure to change it often
- Require Log off of computer systems when staff leave the computer, if an automatic log-off is not an option
- Do not allow the use of external data devices such as USB's or phones to be plugged into work computers
- Do not allow unencrypted laptops to be removed from the premises or left in unprotected areas
- Do not allow unencrypted emails to be sent with patient information

# HIPAA Security Rule Procedures



- Turn computer monitors so they are not visible to people walking by
- Dispose of old equipment and storage devices, such as disks and CDs, properly (documentation must be maintained on all devices ever used within the organization).
- Most importantly, make sure you have an SRA and it is updated annually.

# Summary

- Use the minimum necessary information rule
- Only access PHI needed to do your job.
- Anytime PHI is shared with others, provide only the information the other person or organization needs.
- Understand the rules that limit access to information based on the employee's role within the practice
- Follow the rules about who can access PHI and what types of PHI they are allowed access (for example, a clinical employee who treats patients only needs access to patient health information while the clerical staff may only need to see contact and insurance information).
- Limit computer access and access to the medical records department to only those who need the access to the information



# HIPPA: A Closer Look

Presented By Michelle Bilsky, CHCO, LHRM, MLA, CBA  
Certified HIPAA Compliance Officer

**MedMal**  
**DIRECT**  
Insuring a Healthy Practice